IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

INDIGITAL SOLUTIONS, LLC, *et al.*,	§	
	§	
Plaintiffs,	§	
	§	
v.	§	CIVIL ACTION NO. H-12-2428
	§	
	§	
AHMAD RASHID MOHAMMED, *et al.*,	§	
	§	
Defendants.	§	

MEMORANDUM AND ORDER

Indigital Solutions, LLC and Goran Zinic sued Ahmad Rashid Mohammed and several unidentified individuals and entities for stealing the plaintiffs' personal information and "hijacking" their website's domain name. The plaintiffs allege that they do not know the defendants' true names or addresses and have not been able to serve them. The plaintiffs move for expedited discovery in the form of subpoenas on several third parties. (Docket Entry No. 4). The purpose of the discovery is to obtain the defendants' names and contact information so that service can be attempted. The plaintiffs' motion for expedited discovery is granted, subject to the limits and protective order outlined below.

I. Background

The plaintiffs allege that the defendants used a form of "malicious" computer software called a "Trojan" file to gain unauthorized access to, and steal sensitive information from, the plaintiffs' computer. (Docket Entry No. 1, ¶ 16). The defendants were allegedly able to discover the usernames and passwords for the plaintiffs' Google and GlobalNet email, website hosting, and web domain registration accounts. (*Id.*, ¶ 16). The defendants allegedly used this information to access the plaintiffs' email accounts and locate an email containing Zinic's handwritten signature. (*Id.*, ¶ 19). Around February 20, 2012, the defendants purportedly copied and used that signature to create

a forged "Domain Name Sales Agreement" transferring ownership of the indigitalworks.com domain name from Zinic to Mohammed. (*Id.*, ¶ 20). The defendants allegedly did this by submitting a copy of the forged agreement to OnlineNIC, a domain-name registration company. (*Id.*, ¶ 21). The plaintiffs allege that the defendants' domain-name hijacking has prevented Zinic from controlling and using his domain name and prevented visitors to the plaintiffs' website from viewing it using its original address. The plaintiffs claim that they have lost website traffic and profits. (*Id.*, ¶ 24).

In February or March 2012, the defendants allegedly used the usernames and passwords they stole from the plaintiffs to access the plaintiffs' website hosting account with Hostgator and to download copies of the plaintiffs' website files from the Hostgator servers. (*Id.*, ¶ 25). The defendants then allegedly used these stolen files to create a website that was nearly identical to the plaintiffs' original website. (*Id.*, ¶ 28). The defendants allegedly altered the copycat website's code to link the website to a new Paypal.com account registered under the "indigitalworks" business name but controlled by the defendants. (*Id.*). Visitors who typed "http://www.indigitalworks.com" into their browsers were directed to the defendants' copycat website, and the income earned from the website was paid to the defendants. (*Id.*, ¶ 28).

On March 13, 2012, OnlineNIC suspended the indigitalworks.com domain name in response to the plaintiffs' request. (*Id.*, ¶ 31). The plaintiffs allege that the following day, the defendants launched a distributed denial-of-service attack on the plaintiffs' website by commandeering multiple computers to overload Hostgator's servers. (*Id.*, ¶ 32).

The plaintiffs plead several causes of action, including: (1) violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, for intentionally accessing computers without authorization and with intent to defraud and by obtaining the plaintiffs' financial and other personal information; (2) violations of the Stored Communications Act, 18 U.S.C. § 2701, for intentionally accessing without authorization facilities providing electronic communication services and by altering information

stored in those facilities; (3) conversion, for hijacking the plaintiffs' indigitalworks.com domain name; and (4) trespass to chattels, for interfering with Zinic's use and control over the indigitalworks.com domain name. (*Id*., ¶¶ 34–50).

The plaintiffs move for expedited discovery so that they may serve subpoenas on third parties in order to obtain the defendants' names and contract information. (Docket Entry No. 4).

II. Analysis

Under Federal Rule of Civil Procedure 26(d)(1), "[a] party may not seek discovery from any source before the parties have conferred as required by Rule 26(f), except in a proceeding exempted from initial disclosure under Rule26(a)(1)(B), or when authorized by these rules, by stipulation, or by court order." FED. R. CIV. PROC. 26(d)(1). The plaintiffs ask for an order permitting them to seek discovery from third parties before a Rule 26(f) conference is held. Courts in this circuit have identified several factors to consider in determining whether such early discovery is appropriate, including: (1) whether the plaintiff makes a prima facie showing of harm; (2) the specificity of the discovery request; (3) the absence of alternative means to obtain the subpoenaed information; (4) the necessity of the subpoenaed information to advance the claim; and (5) the user's expectation of privacy. *Well Go USA, Inc. v. Unknown Participants in Filesharing Swarm Identified by Hash* B7FEC872874D0CC9B1372ECE5ED07AD7420A3BBB, 2012 WL 4387420, at *1 (S.D. Tex. Sept. 25, 2012) (citing cases).

The plaintiffs have made a prima facie showing of harm. Title 18 U.S.C. § 1030(g) of the Federal Computer Fraud and Abuse Act (CFAA) prohibits unauthorized access to a "protected computer" for purposes of obtaining information, causing damage, or perpetrating fraud. *Quantlab Techs. Ltd. (BVI) v. Godlevsky*, 719 F. Supp. 2d 766, 774 (S.D. Tex. 2010) (citing § 1030(a)(2), (a)(4), (a)(5)). Although the CFAA is a criminal statute, subsection (g) provides a private right of action under certain circumstances, including when an offense results in a "loss to 1 or more persons

during any 1–year period . . . aggregating in at least $5,000 in value." §§ 1030(g), (c)(4)(A)(I); *Fiber Sys. Int'l, Inc. v. Roehrs*, 470 F.3d 1150, 1156–57 (5th Cir. 2006). The elements of a civil claim under § 1030(a)(5)(A) are: (1) the knowing "transmission" of a "program, information, code, or command"; (2) the transmission is "to a protected computer"; and (3) the transmission causes intentional "damage without authorization." 18 U.S.C. § 1030(a)(5)(A). The plaintiffs allege, among other things, that the defendants transmitted malicious software to their computers without authorization and stole highly sensitive information, including usernames and passwords. The plaintiffs allege that the defendants used this information to hijack the plaintiffs' domain name, causing more than $5,000 in damage. These allegations state a claim under the CFAA and make the necessary prima facie showing of harm.

The plaintiffs' discovery request is sufficiently specific. The plaintiffs ask this court to allow third-party subpoenas to specified recipients seeking particular information. The plaintiffs propose to issue subpoenas to Paypal.com, Hetzner Online AG, and OnlineNIC, requesting the names, mailing addresses, billing addresses, telephone numbers, email addresses, bank names and account numbers, and access logs with logged Internet Protocol addresses that are associated with the defendants' accounts. The plaintiffs state that they will use this information to determine Mohamed's address and the identities and addresses of the Doe defendants. The plaintiffs argue that because Hetzner Online AG and OnlineNIC offer paid services and Paypal requires a linked bank account to withdraw funds, they are likely to have genuine and identifiable information relating to the defendants that allow the plaintiffs to serve them. (Docket Entry No. 5, at 3).

Additionally, the plaintiffs seek to subpoena Yahoo.com and Hotmail.com in order to obtain names, mailing addresses, email addresses, and access logs along with recorded IP addresses for the defendants. The plaintiffs also seek to subpoena Google, GlobalNet and Hostgator.com for access logs to the plaintiffs' own accounts along with recorded IP addresses. The plaintiffs assert that

obtaining the access logs for their own accounts will allow them to send subpoenas to the ISPs associated with the defendants' IP addresses. Those ISPs will in turn be able to identify the owners of the internet service accounts that were used to illegally access the plaintiffs' computers and accounts. The plaintiffs state that the subpoenas to the ISPs will request the names, mailing addresses, billing addresses, telephone numbers, and email addresses for the matching customers. (*Id*. at 4).

It is likely that unless the plaintiffs are permitted to seek pretrial discovery, they will not be able to obtain the information necessary to learn the true names and addresses for the defendants involved in the hijacking. The record reflects that the plaintiffs have made reasonable efforts to obtain information about the defendants through alternative means, without success. According to Zinic's declaration, he does not know the identities of the Doe defendants. The defendants' copycat website did not contain the defendants' contact information. (Docket Entry No. 5-1, ¶¶ 6, 11). The plaintiffs' also justify their need for expedited discovery based on the fact that many ISPs preserve their logs for a limited period of time.

Some of the information that the plaintiffs seek from third parties does not appear necessary at this point, however. The plaintiffs have not identified why they need the defendants' telephone numbers and bank names and account numbers. Due to the sensitive nature of this information, the court declines to permit the plaintiffs to request it at this time. However, the other information that the plaintiffs seek is reasonably calculated to produce the information required to identify and serve the defendants.

In deciding whether and how to permit preservice discovery, courts ordinarily consider the putative defendants' expectations of privacy. *See* FED. R. CIV. P. 45(c)(3)(A) (the "issuing court must quash or modify a subpoena" when it "requires disclosure of privileged or other protected matter, if no exception or waiver applies"). Many of the cases in which plaintiffs request expedited

discovery involve claims that may implicate a defendant's First Amendment rights to anonymous internet communication. *See, e.g.*, *Arista Records, LLC v. Doe*, 604 F.3d 110, 118–19 (2d Cir. 2010) (discussing the putative defendants' First Amendment right to anonymous speech in an infringement case in which a recording company subpoenaed information from ISPs about their users). In this case, it is unclear what, if any, First Amendment-protected activities the defendants might have engaged in. Additionally, the plaintiffs' allegation that Mohammed listed that "Dubai" was his location on his domain registration and the grammatically poor domain name sales agreement also suggest that the putative defendants may reside outside of the United States. *Cf. United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990) (holding that aliens residing outside of the United States did not have Fourth Amendment rights since they lacked a "previous significant voluntary connection with the United States"); *DKT Memorial Fund Ltd. v. Agency for Int'l Dev.*, 887 F.2d 275 (D.C. Cir. 1989) (holding that foreign organizations lacked standing to bring First Amendment claims). These considerations, and the need for discovery to proceed expeditiously so that the plaintiffs are able to subpoena the defendants' ISPs before the sought-after information is deleted, weigh in favor of permitting expedited discovery subject to a protective order.

III. Order

The conference in this matter set for November 16, 2012 is cancelled. The court orders that as follows:

- The plaintiffs may serve Rule 45 subpoenas on Paypal, Hetzner Online AG, and OnlineNIC to obtain the following information about the defendants: their names; mailing addresses; billing addresses; email addresses; and access logs with logged Internet Protocol addresses that are associated with the defendants' accounts. This memorandum and order must be attached to any subpoena. No telephone numbers or bank names and account numbers are to be produced.

- The plaintiffs may serve Rule 45 subpoenas on Yahoo and Hotmail to obtain the following information about the defendants: their names; mailing addresses; email addresses; and access logs with logged Internet Protocol

addresses that are associated with the defendants' accounts. This memorandum and order must be attached to any subpoena. No telephone numbers or bank names and account numbers are to be produced.

- The plaintiffs may serve Rule 45 subpoenas on Google, GlobalNet, and Hostgator to obtain the access logs with any logged Internet Protocol addresses that are associated with the defendants' accounts. This memorandum and order must be attached to any subpoena. No telephone numbers or bank names and account numbers are to be produced.

- If any of the subpoena recipients has responsive information about any of the defendants, it must be disclosed to the plaintiffs. Any information disclosed to the plaintiffs in response to the subpoenas may be used by the plaintiffs only for the purpose of protecting the rights asserted in the complaint. The information disclosed is limited to use by the plaintiffs in this litigation and may not be disclosed other than to counsel for the parties.

- If the subpoenas do not produce sufficient information to identify and serve the defendants with this lawsuit, the plaintiffs may request the court's permission to serve additional subpoenas on the defendants' ISPs and other third parties.

SIGNED on November 15, 2012, at Houston, Texas.

Lee H. Rosenthal
United States District Judge